EXPRESS MAILING LABEL: ER 768177645 US
DATE OF DEPOSIT: 11/18/2003

APPARATUS AND METHOD FOR PHYSICAL LAYER SECURITY AS A ONE-TIME PAD BETWEEN TRANSMITTER AND RECEIVER

FIELD OF THE INVENTION

The invention is related to the field of security; more specifically the invention relates to a system and method for implementing a one-time cryptographic pad between a transmitter and a receiver.

BACKGROUND

All public key crypto-systems, such as PGP and RSA are not theoretically secure, they are only said to be computationally secure. The security of such systems depends on the following problem:

Given a number N, which has only two factors $p1$ and $p2$, both prime numbers,

$N = p1 * p2$ *with* $p1$ *and* $p2$ *prime,*

it is computationally difficult (time consuming) to calculate $p1$ or $p2$. Essentially, there is always a way to break this code by just guessing $p1$, and subsequently dividing N by $p1$. If the result is another prime number (in this case $p2$), the code has been broken. Of course it's very difficult to guess $p1$, because N is normally very large, but if a general algorithm is developed for efficient factorization of any large number, then as a consequence RSA, PGP and other similar public key crypto-systems will become useless.

An additional problem with traditional public key encryption systems is the computational requirements for computing and applying keys. For large keys the computational load can be quite onerous even on a fast personal computer. For hand-held devices having a CPU, such as wireless communications devices, the computational load imposed by even moderate key sizes can be prohibitive.

Public key crypto-systems currently depend on an institution - the trusted authority - that distributes some information vital to the whole system. If this institution is *not secure*, the whole system is not secure. So, the security of all cryptographic exchanges ultimately depends upon the trustworthiness of the trusted authority.

In cryptography, a one-time pad is a system in which a randomly generated secret key is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered. One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.

Typically, a one-time pad is created by generating a string of characters or numbers that will be at least as long as the longest message that may be sent. This string of values is generated in some random fashion - for example, by using a computer program with a random number generator. The values are written down on an electronic pad or database and are distributed to any device that may be likely to send or receive a message. In general, a pad may be issued by a trusted authority as a collection of keys, one for each day in a month, for example, with one key expiring at the end of each day or as soon as it has been used once.

When a message is to be sent, the sender uses the secret key to encrypt each character, one at a time. If a computer is used, each bit in the character (which is usually eight bits in length) is exclusively "OR'ed" with the corresponding bit in the secret key. (With a one-time pad, the encryption algorithm maybe implemented simply by using the

XOR operation.) Where there is some concern about how truly random the key is, it is sometimes combined with another algorithm such as MD5.) This kind of encryption can be thought of as a "100% noise source" used to mask the message. Only the sender and receiver have the means to remove the noise. Once the one-time pad is used, it can't be reused. If it is reused, someone who intercepts multiple messages can begin to compare them for similar coding for words that may possibly occur in both messages.

However, the one-time pad system suffers from the same problem as public key crypto-systems in that a trusted authority must be established to secure and distribute pads.

SUMMARY

Accordingly, a security apparatus and method for implementing a one-time cryptographic pad is disclosed for use by a telecommunication system communicating pair, the communicating pair comprising a first transmitter-receiver and a second transmitter-receiver, the apparatus having devices for sending cryptographic messages from the first transmitter-receiver to the second transmitter-receiver to be decrypted by the second transmitter-receiver, the apparatus comprising: (a) a first storage device in the first transmitter-receiver for storing messages and previous transmissions, or parts thereof, the messages or transmissions previously sent to and received from the second transmitter-receiver of the pair; (b) a second storage device for storing transmissions and messages or parts thereof, the transmissions and messages previously sent to and received from the first transmitter-receiver of the pair; (c) a plurality of cryptographic devices in the first transmitter-receiver, each of the cryptographic devices having a reference known to the first transmitter-receiver; (d) the same plurality of cryptographic devices with references also known to the second transmitter-receiver; (e) a selection device in the first transmitter-receiver for selecting and retrieving a transmission or message or a part thereof previously sent to the second transmitter-receiver; (f) a state computation device in the first transmitter-receiver for computing a random number as a function of a reference over one of the plurality of cryptographic devices known to the communicating pair, the function also being over a previous transmission or message sent to the second

transmitter-receiver, the set of states known to the communicating pair; (g) a message sending device in the first transmitter-receiver for creating and sending a message to the second transmitter-receiver, the message containing the a previously sent transmission or message, or some part thereof, sent by the first transmitter receiver, and a reference to a transmission or message previously sent to the first transmitter-receiver by the second transmitter-receiver, the message sending device further encrypting the message using a cryptographic device randomly selected by the first transmitter-receiver; (h) a message receiving device in the second transmitter-receiver for receiving the message sent by the first transmitter-receiver, the message receiving device also extracting the encrypted previous transmission or message or part thereof sent by the first transmitter-receiver, and further extracting the reference sent by the first transmitter-receiver; (i) a cryptographic device reference decoder in the second transmitter-receiver for discovering the reference to the cryptographic device randomly selected by the first transmitter-receiver; (j) a reference decoding device in the second transmitter-receiver for controlling the cryptographic device associated with the reference discovered by the cryptographic reference decoder, the cryptographic decoding device applying the referenced cryptographic device to decrypt the previous transmission or message or part thereof sent by the first transmitter-receiver and to decrypt the reference to a transmission or message previously sent by the second transmitter receiver; (k) a message selection device in the second transmitter-receiver for selecting a previous transmission or message or a part thereof, stored in the second storage device, and for encrypting the transmission or message or a part thereof, selected, the message or part thereof encrypted using the encryption device associated with the reference discovered, and for sending the encrypted selected message or part thereof to the first transmitter-receiver; (l) a confirmation device in the first transmitter-receiver for confirming the correct reference was found by the second transmitter-receiver, and for confirming the correct transmission message previously sent by the second transmitter-receiver, the confirmation device using the cryptographic device associated with the cryptographic device reference sent to the second transmitter-receiver to decrypt the encrypted selected transmission or message sent by the second transmitter-receiver, and to evaluate the contents of the decrypted selected transmission or message sent by the second transmitter-receiver and to signal

confirmation of no-confirmation; whereby the first transmitter-receiver, when sending an encrypted message to the second transmitter-receiver: (a) randomly selects an encryption device associated with a reference, and randomly selects a reference to a transmission or message previously received from the second transmitter-receiver; (b) using the randomly selected cryptographic device encrypts the previous transmission or message sent by the first transmitter-receiver and the reference to a previously sent by the second transmitter-receiver; (c) sends the encrypted message to the second transmitter-receiver; (d) the second transmitter-receiver discovers the cryptographic device randomly selected by the first transmitter-receiver and discovers the reference to the previous message sent; (e) the second transmitter-receiver using the discovered encryption device encrypts the referenced transmission or message or some part thereof sent to the first transmitter-receiver, and sends the encrypted referenced transmission or message or part thereof the first transmitter-receiver; and, (f) the first transmitter-receiver confirms the correctness of the contents of the encrypted message sent by the second transmitter-receiver and confirms the security of a transmission to the second transmitter-receiver.

The invention is seen to have a number of objects and advantages, the first object and advantage is that the invention implements a one-time pad between communicating pairs; the advantages and security benefits of a one-time pad well-known.

A second advantage is that by using the state computation device with information known only to the communicating pair, the state computation device causing the cryptographic synchronization of the communicating pair, traditional cryptographic security can be made exponentially more difficult to break.

These advantages plus other advantages and benefits will be seen from reading of the detailed description and drawings that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows an exemplary environment for implementing a method of the invention.

Figure 2 is a flow diagram of the steps of a method used by a first transmitter-receiver in establishing a one-time cryptographic pad in collaboration with a second transmitter-receiver.

Figure 3 is a flow diagram of the steps of a method used by the second transmitter-receiver in establishing a one-time pad in collaboration with the first transmitter-receiver.

Figure 4 is a flow diagram of additional steps of a method used by the first transmitter-receiver in establishing a one-time cryptographic pad in collaboration with the second transmitter-receiver.

DETAILED DESCRIPTION

An environment for practicing the invention

The invention is practiced by a communicating pair, the communicating pair comprising a first transmitter-receiver and a second transmitter-receiver communicating over a communications media or a communications facility, such as cable, wireless or optical transmission means.

The communicating pair are furnished with a plurality of cryptographic devices for encrypting and decrypting messages exchanged. The cryptographic devices are selected from the group consisting of : (a) plurality of pseudo-random number generators (for generating random keys that are exclusively or'ed with the message); (b) a plurality of elliptic curve cryptosystems; (c) a plurality of discrete-logarithm (RSA) cryptosystems; and, (d) a plurality of so-called symmetric-key cryptosystems.

An exemplary method for establishing a one-time cryptographic pad between a communicating pair

Under control of logic in the first transmitter-receiver, a message is prepared to transmit to the second transmitter-receiver. Prior to sending the message, the first transmitter-receiver collaborates to establish a one-time cryptographic pad for encrypting the message to be sent. Collaboration comprises the communicating pair negotiating

agreement on a cryptographic device to be used to encrypt and decrypt exchanged messages.

During the process of preparing to transmit and receive messages, the communicating pair engage in a private protocol to establish a connection, choose parameters required to modulate-demodulate signals, and to synchronize communications. During this process, the communicating pair exchange information regarding internal data, as stored in internal data structures, and states that are private and common to the communicating pair and are independent of the content of transmitted messages. Either private internal data or some portion of a previously exchanged message is used by the communicating pair to negotiate a one-time pad. This information, whether a message, part thereof, or private internal data is hereafter is called a transmission, to distinguish from messages that are sent in response to a using device of the communicating pair.

With reference to Figure 2, the first transmitter-receiver executes the first of a series of steps 2000 to set up the pad. The first transmitter-receiver 2100 randomly selects a reference to one of the plurality of encryption devices. For example, the reference may a number that designates the cryptographic device, or a pointer to a cryptographic software object having methods called to encrypt and decrypt data. The first transmitter-receiver retrieves a previous transmission received from the second transmitter-receiver 2200, then 2300 encrypts the previously received transmission using randomly selected encryption device.

It will be appreciated that by sending a previous transmission received from the second transmitter-receiver, the first transmitter-receiver is providing at least some verification of its authenticity with respect to a secure communications channel. Furthermore, the previous transmission is selected from the group consisting of (a) the last message sent by the second transmitter-receiver; (b) a predetermined portion of the last message sent by the second transmitter-receiver; and (c) prespecified internal data that is generated by the communicating pair, that is independent of message content.

The first transmitter-receiver 2400 randomly selects a reference to some previous transmission sent by the first transmitter-receiver to the second transmitter-receiver, then 2500 encrypts the reference and constructs a message 2600, which is sent to the second

transmitter-receiver. The previous transmission in this case is selected from the group consisting of: (a) a previous referenced message sent by the second transmitter-receiver; (b) a predetermined portion of a previous referenced message sent by the second transmitter-receiver; and (c) prespecified internal data that is generated by the communicating pair, that is independent of message content.

When the second transmitter-receiver receives the encrypted transmission from the first transmitter-receiver, the second transmitter-receiver executes the steps 3000 shown in Figure 3.

With reference to Figure 3000, the second transmitter-receiver 3100 receives the encrypted transmission, and discovers the cryptographic device used by the first. transmitter-receiver. Discovery can be made in several ways, with one example being the second transmitter-receiver sequentially uses all its cryptographic devices, in turn, to decrypt the transmission received from the first transmitter-receiver. The second transmitter-receiver will have identified the cryptographic device used by the first transmitter-receiver when it is able to recover the transmission previously sent by the first transmitter-receiver that is known to second transmitter-receiver. Since the number of cryptographic devices is small in number, for example, less than twenty, the number of computational steps is relatively small to discover the cryptographic device used by the first transmitter-receiver, by sequential trial and error, although other methods are conceivable.

With respect to Figure 3, 3300 having discovered the cryptographic device used by the first transmitter-receiver, the second transmitter-receiver decrypts the reference to a previous transmission sent by the second transmitter-receiver, and using the reference, accesses the transmission previously sent by the second transmitter-receiver. At this point, the second transmitter-receiver can respond to verify its authenticity by responding with the referenced transmission, or the second transmitter-receiver can respond by challenging the first transmitter-receiver to further provide evidence of its authenticity.

With reference to 3400, if the second transmitter-receiver challenges the first transmitter-receiver, it prepends a code indicating request for further evidence of authenticity and then appends a reference to a previous transmission that the second transmitter-receiver requests to be sent by the first transmitter-receiver. The code and

reference are encrypted using the an encryption device randomly selected by the second transmitter-receiver and sent to the first transmitter-receiver. In this case the roles of the first and second communicating pairs are reversed.

If the first transmitter-receiver authenticity is accepted, the second transmitter-receiver 3500 encrypts the previously sent transmission and 3600 sends the encrypted transmission to the first transmitter-receiver.

When the first transmitter-receiver receives the encrypted previous transmission from the second transmitter-receiver, the first transmitter-receiver performs the steps 4000 shown in Figure 4.

With reference to Figure 4, 4100 the first transmitter-receiver receives the encrypted transmission from the second transmitter-receiver, then using the encryption device selected by first transmitter-receiver, the transmission previously sent by the second transmitter-receiver is decrypted and 4300 is confirmed or disconfirmed by the first transmitter-receiver. The state of the confirmation is reported 4400, and if confirmed, the one-time pad, or cryptographic device is used to encrypt and transmit the current message.

DISCLOSURE SUMMARY

An apparatus and method for implementing a one-time cryptographic pad between a communicating pair has been disclosed. It will be appreciated and understood that the invention has been described in exemplary form and that there are numerous variations and changes that will be obvious to one skilled in the art of the field of the invention.